deepwatch™

CUSTOMER SUCCESS STORY

RJ O’Brien Financial Services Case Study

ABOUT THE COMPANY

RJ O’Brien & Associates LLC is the oldest and largest independent futures brokerage and clearing firm in the United States. RJO offers the latest in order entry technology coupled with 24-hour execution and clearing on every futures exchange worldwide. Clearing more than 100,000 client accounts, the firm provides a full range of services to the industry’s largest global network of introducing brokers (IBs) and to commercial, institutional, international, and individual clients.

THE CHALLENGE

RJ O’Brien faced three security challenges: a shift to remote work, concerns about ransomware as well as skills and resource limitations.

In 2020, traders who traditionally worked in-office due to technical and regulatory issues needed to shift to remote work. This presented a new set of challenges for RJ O’Brien’s IT and security teams, such as deploying and securing more equipment. To support the shift to a remote workforce, RJ O’Brien moved to cloud-based tools.

Ransomware was of particular concern. With the increase in ransomware targeting mid-market companies, Woods wanted to proactively implement a solution to decrease time to detect, before RJ O’Brien experienced an attack. Because, “if a Ransomware attack isn’t caught in a short enough period of time, they are costly and small businesses are at high risk.”

Without 24/7 monitoring, after-hour alerts were a constant struggle for the RJO in-house team. After trying different strategies for managing off-hour alerts, Woods found himself still lacking confidence that the alerts were being reviewed and responded to with the expertise required to determine whether a) to call him in the middle of the night, or b) whether it could wait till morning.

While Woods recognized that RJ O’Brien needed round-the-clock monitoring, he lacked the staff and budget to implement the required 3 shifts, with 3 to 5 employees per shift. With an alert-fatigued in-house security team and a limited budget, this was not doable. Knowing his budget couldn’t cover a best-in-class SIEM, Woods opted instead for the less-ideal, but free, open-source SIEM. However, that solution required significant engineering resources to maintain. He looked at managed SIEM options but could not find a provider for his open-source SIEM. In his experience, all managed SIEM providers either used proprietary “black box” tools, or required him to invest in expensive SIEM technology.

Woods found himself in the tough position no CISO wants to be in—knowing there were gaps in the RJ O’Brien’s security posture, but lacking the staff and budget to fully resolve the gaps.

ENTERPRISE DETAILS

Who: RJ O’Brien

Industry: Financial Services

Location: Chicago, IL

Company Size: 520

Customer Since: June 2021

Security Team Size: 3

“We are able to talk with the same dedicated account manager with every interaction, who takes the time to understand our environment and why certain alerts hold more weight than others. They feel like an extension of our team.”

JOHN WOODS,
GLOBAL CISO, RJ O’BRIEN

WHY WORK WITH DEEPWATCH

Get 24/7/365 Managed Detection and Response with Human Analysts & a Named Account Manager. The named account manager learned the nuances of RJ O'Brien's environment. This saves the team time. If there was a new person every time, those nuances wouldn't be remembered.

If you don't have the budget for an in-house SOC, Deepwatch offers the benefits of a SOC with best-in-class technology, without needing to buy the technology stack.

> **"Other outsource providers we looked at standardize on expensive tools, so if I want to work with them, I need to buy the expensive tool to work with them... the Deepwatch service feels personal. We have created a relationship with a Deepwatch person who knows our environment. It's better than we expected."**
>
> **JOHN WOODS,**
> GLOBAL CISO, RJ O'BRIEN

SOLUTION

Deepwatch MDR Essentials offered RJ O'Brien the critical 24/7 monitoring it needed at a price that fit their budget.

RJ O'Brien implemented Deepwatch Managed Detection and Response (MDR) to relieve the alert fatigue and constant pressure burdening the RJ O'Brien security team. Woods liked the speed and ease of deployment required to get Deepwatch MDR up and running. Using an API integration to connect into RJ O'Brien's Microsoft Cloud, Deepwatch quickly gained visibility into 100% of what the internal team sees, without the need to deploy agents onto each and every endpoint and server. Woods liked that the Deepwatch MDR solution uses human analysts to review and prioritize alerts, and provides him with a dedicated account manager.

Woods highlighted the importance of the human element that comes with Deepwatch MDR: "We are able to talk with the same dedicated account manager with every interaction, who takes the time to understand our environment and why certain alerts hold more weight than others. They feel like an extension of our team."

OUTCOME

The primary value Deepwatch MDR provides is risk mitigation. With security gaps filled, RJ O'Brien has a stronger security posture. Today, Woods has moreconfidence in the organization's security, knowing all threats are being monitored and prioritized. For a small company with a team in one timezone, this is essential. Implementing Deepwatch MDR also increased productivity. By filling an otherwise unfilled gap, the RJ O'Brien team is able to focus on tasks they previously did not have time to do.

Significant cost avoidance by going with the Deepwatch MDR service. Woods said that the "alternative would be to spend 2x as much, plus needing SOC engineers at $100k each and it might be almost as good... we spend less than hiring one SOC professional and we get the benefit of best-in-class technology." Since Deepwatch MDR is implemented and connected to the cloud, deployment was fast and easy, taking only one hour from start to finish.

Improved work-life balance for the team. With confidence in the 24/7 monitoring provided by Deepwatch, the RJ O'Brien security team is able to enjoy a better work-life balance. Woods shared that, "[Thanks to Deepwatch], my team and I are able to enjoy time with our families without having to check our emails all night."

deepwatch™

ABOUT DEEPWATCH

Deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, Deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com